# REMARKS

Herein, the "Action" or "Office Action" refers to the Office Action dated 7/1/2004.

Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-15 and 18-35 are presently pending. Claims amended herein are 18, 19, and 29. Claims withdrawn or cancelled herein are 16 and 17. New claims added herein are none.

## Substantive Claim Rejections

### Claim Rejections under §§ 102 & 103

The Office rejects all of the pending claims under §102 and/or §103. For the reasons set forth below, the Office has not shown that cited references anticipate (under §102) the rejected claims. For the reasons set forth below, the Office has not shown made a *prima facia* case showing that the rejected claims are obvious (under §103). Accordingly, Applicant respectfully requests that the rejections be withdrawn and the case be passed along to issuance.

The Office's rejections are based upon the following references:

- **Olden:** *Olden.,* US Patent No. 6,460,141 (issued 10/1/2002); and/or

- **McNabb:** *McNabb et al.,* US Patent No. 6,289,462 (issued 9/11/2001).

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

14

*0907040945 G:\MS1-0\679us\MS1-679us.m01.doc*

atty: Kassey C. Christie

## Overview of the Application

The Application describes a domain-authentication aware technology for managing credentials. In other words, an authentication by one resource in a trust network enables automatic (without manual user input) authenticated access to all resources in that trust network.

With an implementation of this technology, concurrent authentications with multiple independent networks (e.g., domains) may be established and maintained.

With an implementation of this technology, a credential manager provides a credential model retrofit for legacy applications that only understand the password model. The manager marshals high-level credentials (such as a certificate) so that the high-level credential appears to be a low-level credential (such as a user/password) to legacy applications.

With an implementation of this technology, a credential manager provides a mechanism where the application is only a "blind courier" of credentials between the trusted part of the OS to the network and/or network resource. The manager fully insulates the application from "read" access to the credentials.

## Cited References

The Office cites **Olden** as its primary references in its anticipation- and obviousness-based rejections. The Office cites **McNabb** as its secondary reference in its obviousness-based rejection.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

lee@hayes

## Olden

Olden describes a security and access management technology for Web-enabled and non-Web-enabled applications and content on a computer network. Olden describes a management model which brings together disparate infrastructure components, consolidates multiple security policies, and embraces both Web and emerging Internet technologies to properly address the security requirements of the Web.

Olden describes a uniform access management model to address the specific problems facing the deployment of security for the Web and non-Web environment. Unified access management consists of strategic approaches to unify all key aspects of Web and non-Web security policies, including access control, authorization, authentication, auditing, data privacy, administration, and business rules. Unified access management also addresses technical scalability requirements needed to successfully deploy a reliable unified Web and non-Web security system.

Olden describes the technology required to support these key factors as they relate to Web and non-Web security. The described system operates in combination with network and system security tools such as firewalls, network intrusion detection tools, and systems management tools to provide comprehensive security for the Web-enabled enterprise.


## McNabb

McNabb describes a technology for providing a trusted server which controls access to the execution of processes by applying file level extended sensitivity label attributes. The attributes are utilized to restrict

execution of processes that are requested by comparing the extended attributes in addition to using standard file permission authorization.

## Anticipation Rejections

### Based upon Olden

The Office rejects claims 1-2, 4-8, 10-24, and 26-35 under USC § 102(e) as being anticipated by **Olden**. Applicant respectfully traverses the rejections of these claims. Based on the reasons given below, Applicant asks the Office to withdraw its rejection of these claims.

*Claim 1*

This claim recites:

- **obtaining a request for a high-level credential from a legacy application;**
- **marshalling the requested credential;**
- **returning the marshaled credential to the application.**

The Office cites col. 25, lines 29-39 of **Olden** and, by doing so, indicates that the cited portion of the reference discloses all of the elements and features of this claim.

However, the Applicant submits that the Office has not identified, with particularity, where each feature and element of this claim is found in the cited passage of the reference. Furthermore, the Office has not

provided any reasoning, explanation, or rationale as to its assertion that the cited portions of **Olden** disclose all of each feature and element of this claim,

High-Level Credential

The cited portion (col. 25, lines 29-39) of **Olden** reads:

> For example, consider that user Steve may have one username/password for Web applications and a different username and password for a legacy application. Single sign on from the Web to the legacy application can be accommodated by storing the user's legacy credentials as user properties for Steve such as legacy_username and legacy_password in the entitlements database 32. The legacy Web application would then query the API and request the legacy_username and legacy_password for ct_username=steve. The results can then be transferred to the legacy application to be used in the logon procedure. Since this is performed programmatically, the user is not aware of the second logon process. To the user, it seems as if he or she only logged onto the Web site once.

A non-password authorization model (e.g., a X.509 Certificates) utilizes *high-level credentials*. However, most legacy applications have provisions for only the traditional username/password authorization model which is an example of a *low-level credential*.

This distinction between high- and low-level credentials is discussed through-out the Application. For example, this distinction is noted in the following section quoted the 3rd paragraph of the "Summary" on p. 5 of the Application:

18

With an implementation of this technology, a credential manager provides a credential model retrofit for legacy applications that only understand the password model. The manager marshals high-level credentials (such as a certificate) so that the high-level credential appears to be a low-level credential (such as a user/password) to legacy applications.

This claim recites (with emphasis added): "obtaining a request for a *high-level credential* from a legacy application."

Applicant submits the **Olden** does not do this. Instead, with **Olden**, authorization to access a first set of functionality based upon a traditional low-level credential (username/password pair) allows for automatic authorized access to a second set of functionality. This automatic secondary access is predicated upon the first authorization and is accomplished by retrieval of a databased low-level credential for this authorized access to a second set of functionality.

While Olden handles multiple credentials and allows for automatic access to additional functionality based upon authorization via only one set of credentials, Olden ONLY handles low-level credentials. It only handles the traditional username/password pair model. Applicant submits that Olden never discloses utilizing *high-level credentials*. Applicant submits that Olden never discloses utilizing certificates.

Therefore, Applicant submits that **Olden** does not disclose "a request for a high-level credential," as recited in this claim.

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

19

0907040945 G:\MS1-0679us\MS1-679us.m01.doc
atty: Kasey C. Christslo

PAGE 22/41 * RCVD AT 10/7/2004 1:18:47 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:509 323 8979 * DURATION (mm-ss):10-24

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324.9256
F: 509.323-8979
www.leehayes.com

lee@hayes

<u>Marshalling</u>

Furthermore, Olden does not disclose "marshaling" as recited in this claim. Specifically, this claim recites (with emphasis added): *"marshalling the requested [high-level] credential; returning the marshaled credential* to the application."

Pages 12-15 of the Application describe the concepts of "marshalling" and "marshaled credentials" in some detail. In the first paragraph on p. 12, this definition is provided: "Marshaling is the mechanism by which a description of a non-password credential can be passed to the TCB [Trusted Computing Base] using an interface designed to support only password credentials."

Therefore, Applicant submits that **Olden** does not disclose the concepts of "marshalling" and "marshaled credentials," as recited in this claim.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

<u>Claims 2-7</u>

These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

20

0907040945 G:\MS1-0167Bus\MS1-679us.m01.doc
atty: Kasey C. Christie

PAGE 23/41 * RCVD AT 10/7/2004 1:18:47 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:509 323 8979 * DURATION (mm-ss):10-24

submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

## Claim 8

The Office indicates that this claim incorporates substantially similar subject matter as claim 1 and is rejected along the same rationale.

If this is true, the Applicant submits that this claim is allowable for same reasons given above as to why claim 1 is allowable.

While the Office's assertion (that this claim incorporates substantially similar subject matter as claim 1) may or may not be true, Applicant asserts that this independent claim is patentable different than claim 1; and therefore, it deserves to be examined on its own.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## Claims 9-12

These claims ultimately depend upon independent claim 8. As discussed above, claim 8 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

## Claim 13

The Office indicates that this claim incorporates substantially similar subject matter as claim 1 and is rejected along the same rationale.

If this is true, the Applicant submits that this claim is allowable for same reasons given above as to why claim 1 is allowable.

While the Office's assertion (that this claim incorporates substantially similar subject matter as claim 1) may or may not be true, Applicant asserts that this independent claim is patentable different than claim 1; and therefore, it deserves to be examined on its own.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## Claims 14-15

These claims ultimately depend upon independent claim 13. As discussed above, claim 13 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

lee@hayes

*Claims 16 and 17*

Applicant has canceled these claims. Therefore, the rejection is moot.

*Claim 18*

With the cited portions of Olden in brackets, this claim recites:

- a **trusted computing base (TCB) that has full access to persisted credentials, the TCB being configured to interact with an untrusted computing layer (UTCL) that accesses the persisted credentials via the TCB;**

- the **TCB comprises:**

  o a **credential management module configured to receive requests from the UTCL for a high-level credential for a resource,** [col. 3, lines 39-61] **the high-level credential being associated with a user;**

  o a **credential database associated with the user, wherein credentials are persisted within the database;**

  o the **credential management module being configured to retrieve credentials from the database.** [col. 4, lines 27-34]

However, the Applicant submits that the Office has not identified, with particularity, where each feature and element of this claim is found in

lee@hayes

1  the cited passage of the reference.    Furthermore, the Office has not

2  provided any reasoning, explanation, or rationale as to its assertion that the

3  cited portions of **Olden** disclose all of each feature and element of this

4  claim.

5  The cited portions of **Olden** read:

6

7  The security and access management system of the present

8  invention, generally indicated by the numeral 10 in FIG. 1, is a

   highly scalable, reliable, and configurable security architecture. As

9  shown in FIG. 1, the architecture for the security and access

10  management system 10 comprises five main components: at least

11  one authorization component 12; an entitlements (database) server

    component 14; an API server 16; an administrative client

12  (graphical user interface) 18; and at least one enabled Web server

13  20 connected to the remainder of the computer network, for

14  example, over the Internet. The first three components are server-

15  side components. Each of the server-side components will now be

    described in more detail.

16

17  The authorization component 12 performs authorization

18  processing on behalf of either an enabled Web server 20 or an API

    client 22. The authorization component 12 comprises an

19  authorization server 24. Preferably, as shown in FIG. 1, the

20  authorization component 12 comprises a plurality of authorization

21  servers 24A, 24B, 24C and at least one authorization dispatcher 26.

22  In order to avoid a single point source of failure, a plurality of

23  authorization dispatchers 26A, 26B also preferably comprises the

    authorization component 12. [col. 3, lines 39-61]

24

25

Left margin: 421 West Riverside, Suite 500 Spokane, WA 99201  P: 509.324-9256  F: 509.323-8979  www.leehayes.com  lee@hayes

...

The entitlements server component 14 performs database processing on behalf of at least one entitlements manager administrative client 18 and the API server 16. In addition, the entitlements server component 14 also forwards requests from the entitlements manager administrative client 18 and API server 16 to the authorization servers 24A, 24B, 24C comprising the authorization component 12. [col. 4, lines 27-34]

A non-password authorization model (e.g., a X.509 Certificates) utilizes *high-level credentials*. However, most legacy applications have provisions for only the traditional username/password authorization model which is an example of a *low-level credential.*

This distinction between high- and low-level credentials is discussed through-out the Application. For example, this distinction is noted in the following section quoted the 3rd paragraph of the "Summary" on p. 5 of the Application:

With an implementation of this technology, a credential manager provides a credential model retrofit for legacy applications that only understand the password model. The manager marshals high-level credentials (such as a certificate) so that the high-level credential appears to be a low-level credential (such as a user/password) to legacy applications.

This claim recites (with emphasis added): "a credential management module configured to receive requests from the UTCL for a *high-level credential* for a resource."

Applicant submits the **Olden** does not do this. Instead, with **Olden**, authorization to access a first set of functionality based upon a traditional low-level credential (username/password pair) allows for automatic authorized access to a second set of functionality. This automatic secondary access is predicated upon the first authorization and is accomplished by retrieval of a databased low-level credential for this authorized access to a second set of functionality.

While Olden handles multiple credentials and allows for automatic access to additional functionality based upon authorization via only one set of credentials, Olden ONLY handles low-level credentials. It only handles the traditional username/password pair model. Applicant submits that Olden never discloses utilizing *high-level credentials*. Applicant submits that Olden never discloses utilizing certificates.

Therefore, Applicant submits that **Olden** does not disclose "a request for a high-level credential," as recited in this claim.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

26

0907040945 G:\MS1-0679us\MS1-679us.m01.doc
atty: Kasey C. Christie

## Claims 19-22

These claims ultimately depend upon independent claim 18. As discussed above, claim 18 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

## Claim 23

The Office indicates that this claim incorporates substantially similar subject matter as claim 1 and is rejected along the same rationale.

If this is true, the Applicant submits that this claim is allowable for same reasons given above as to why claim 1 is allowable.

While the Office's assertion (that this claim incorporates substantially similar subject matter as claim 1) may or may not be true, Applicant asserts that this independent claim is patentable different than claim 1; and therefore, it deserves to be examined on its own.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## Claim 24

The Office indicates that this claim incorporates substantially similar subject matter as claim 8 and is rejected along the same rationale.

If this is true, the Applicant submits that this claim is allowable for same reasons given above as to why claim 1 is allowable.

While the Office's assertion (that this claim incorporates substantially similar subject matter as claim 8) may or may not be true, Applicant asserts that this independent claim is patentable different than claim 1; and therefore, it deserves to be examined on its own.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## Claims 25-28

These claims ultimately depend upon independent claim 24. As discussed above, claim 24 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

_Claim 29_

This claim recites:

- a request obtainer configured to obtain a request for a high-level credential to authenticate the user to access a resource within the network, wherein the resource requires an appropriate credential before the user may access the resource;

- a credential retriever configured to retrieve the appropriate high-level credential from a database of credentials;

- a credential marshaller configured to generate a representation of the high-level credential that is formatted as a low-level credential so that it appears to be a conventional username/password pair;

- a credential returner configured to return the appropriate marshaled credential to the resource within the network, so that the resource allows the user to access such resource;

- wherein the obtainer, retriever, marshaller, and returner are further configured to operate without user interaction.

The Office cites col. 3, lines 39-61, col. 4, lines 27-34, and col. 25, lines 39-41 of Olden and, by doing so, indicates that the cited portion of the reference discloses all of the elements and features of this claim.

However, the Applicant submits that the Office has not identified, with particularity, where each feature and element of this claim is found in the cited passage of the reference. Furthermore, the Office has not

provided any reasoning, explanation, or rationale as to its assertion that the cited portions of **Olden** disclose all of each feature and element of this claim,

### High-Level Credential

A non-password authorization model (e.g., a X.509 Certificates) utilizes *high-level credentials*. However, most legacy applications have provisions for only the traditional username/password authorization model which is an example of a *low-level credential*.

This distinction between high- and low-level credentials is discussed through-out the Application. For example, this distinction is noted in the following section quoted the 3ʳᵈ paragraph of the "Summary" on p. 5 of the Application:

> With an implementation of this technology, a credential manager provides a credential model retrofit for legacy applications that only understand the password model. The manager marshals high-level credentials (such as a certificate) so that the high-level credential appears to be a low-level credential (such as a user/password) to legacy applications.

This claim recites (with emphasis added): "a request obtainer configured to obtain a request for a *high-level credential* to authenticate the user to access a resource within the network."

Applicant submits the **Olden** does not do this. Instead, with **Olden**, authorization to access a first set of functionality based upon a traditional

30

low-level credential (username/password pair) allows for automatic authorized access to a second set of functionality. This automatic secondary access is predicated upon the first authorization and is accomplished by retrieval of a databased low-level credential for this authorized access to a second set of functionality.

While Olden handles multiple credentials and allows for automatic access to additional functionality based upon authorization via only one set of credentials, Olden ONLY handles low-level credentials. It only handles the traditional username/password pair model. Applicant submits that Olden never discloses utilizing *high-level credentials*. Applicant submits that Olden never discloses utilizing certificates.

Therefore, Applicant submits that **Olden** does not disclose "a request for a high-level credential," as recited in this claim.

Marshalling

Furthermore, Olden does not disclose "marshaling" as recited in this claim. Specifically, this claim recites: "a credential marshaller configured to generate a representation of the high-level credential that is formatted as a low-level credential so that it appears to be a conventional username/password pair."

Pages 12-15 of the Application describe the concepts of "marshalling" and "marshaled credentials" in some detail. In the first paragraph on p. 12, this definition is provided: "Marshaling is the mechanism by which a description of a non-password credential can be

passed to the TCB [Trusted Computing Base] using an interface designed to support only password credentials."

Therefore, Applicant submits that **Olden** does not disclose the concepts of "marshalling" and "marshaled credentials," as recited in this claim.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## _Claims 30-31_

These claims ultimately depend upon independent claim 29. As discussed above, claim 29 is allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

32

0907040945 G:\MS1-0679us\MS1-679us.m01.doc
atty: Kasey C. Christin

## *Claim 32*

This claim for an application programming interface (API) method recites:

- receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, Context, AuthFlags, and Flags;
- parsing the call to retrieve the parameters to determine a specified resource;
- obtaining a credential;
- associating the credential with the specified resource;
- persisting the credential into a database while maintaining the credential's association with the specified resource.

The Office cites col. 3, lines 39-61 and col. 9, line 27 through col. 10, line 36 of **Olden** and, by doing so, indicates that the cited portion of the reference discloses all of the elements and features of this claim.

However, the Applicant submits that the Office has not identified, with particularity, where each feature and element of this claim is found in the cited passage of the reference. Furthermore, the Office has not provided any reasoning, explanation, or rationale as to its assertion that the cited portions of **Olden** disclose all of each feature and element of this claim,

In particular, the Office has not identified, nor can Applicant find, where **Olden** discloses "receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, Context, AuthFlags,

and Flags." No where does **Olden** disclose a call with these particular set of parameters.

Furthermore, Applicant submits that **Olden** does not disclose the all of the steps of this method (parsing a call; obtaining a credential; associating; and persisting) generally or specifically. For example, **Olden** does not disclose "associating the [obtained] credential with the specified resource."

If **Olden** does disclose these things, Applicant asks that the Office identify where it discloses it with particularity.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

## *Claim 33*

This claim ultimately depends upon independent claim 32. As discussed above, claim 32 is allowable.

In addition to its own merits, this dependent claim is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of this dependent claim because its base claim is allowable.

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004
34
0907040945 G:\MS1-01679us\MS1-679us.m01.doc
atty: Kasey C. Christie

PAGE 37/41 * RCVD AT 10/7/2004 1:18:47 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:509 323 8979 * DURATION (mm-ss):10-24

## _Claim 34_

This claim for an application programming interface (API) method recites:

- **receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, UserName, Password, and Flags;**

- **parsing the call to retrieve the parameters to determine a requesting application;**

- **obtaining a low-level credential from a user, wherein such credential includes a username and a password;**

- **returning the low-level credential to the requesting application.**

The Office cites col. 9, line 27-45 and col. 7, lines 26-41 of **Olden** and, by doing so, indicates that the cited portion of the reference discloses all of the elements and features of this claim.

However, the Applicant submits that the Office has not identified, with particularity, where each feature and element of this claim is found in the cited passage of the reference. Furthermore, the Office has not provided any reasoning, explanation, or rationale as to its assertion that the cited portions of **Olden** disclose all of each feature and element of this claim,

In particular, the Office has not identified, nor can Applicant find, where **Olden** discloses "• receiving a CredUI-promptfor-credentials call having a set of parameters comprising a TargetName, UserName,

Margin left side:
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

lee@hayes

Password, and Flags." No where does **Olden** disclose a call with these particular set of parameters.

As shown above, **Olden** does not disclose all of the claimed elements and features of the claim. Accordingly, Applicant asks the Office to withdraw its rejection of this claim.

*Claim 35*

This claim ultimately depends upon independent claim 34. As discussed above, claim 34 is allowable.

In addition to its own merits, this dependent claim is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of this dependent claim because its base claim is allowable.

# Obviousness Rejections

## Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

Applicant disagrees with the Office's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a *prima facie* case have not been met.

## Based upon Olden and McNabb

The Office rejects 3, 9, and 25 under USC § 103(a) as being unpatentable over **Olden** as modified by **McNabb**. Applicant respectfully traverses the rejections of these claims. Applicant asks the Office to withdraw its rejection of these claims.

These claims ultimately depend upon independent claims 1, 8, and/or 24. As discussed above, these claims are allowable.

In addition to its own merits, each of these dependent claims is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each of these dependent claims because its base claim is allowable.

## Dependent Claims

In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant submits that the Office withdraw the rejection of each dependent claim where its base claim is allowable.
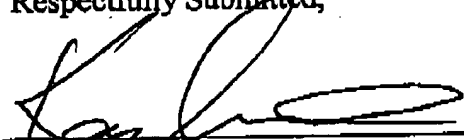
421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-6979
www.leehayes.com

lee@hayes

## Conclusion

All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the Office is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: /0-7-04

By: _____

Kasey C. Christie
Reg. No. 40559
(509) 324-9256 x232
kasey@leehayes.com
www.leehayes.com

421 West Riverside, Suite 500
Spokane, WA 99201
P: 509.324-9256
F: 509.323-8979
www.leehayes.com

lee⊗hayes

Serial No.: 09/757,058
Atty Docket No.: MS1-679us
RESPONSE TO OFFICE ACTION DATED 7/1/2004

38

0907040945 G:\MS1-0\679us\MS1-679us.m01.doc

atty: Kasey C. Christie